Appunti di Algebra (II mod)

Erika Paola Spinosi

Appunti tratti dalle lezioni del professore Lino Di Martino.

Indice

Capitolo 1. Corpi e campi 5
1.1. Estensioni polinomiali di UFD 8
1.2. Polinomi in più variabili 11
1.3. Radici di polinomi 12
1.4. Proprietà universale di $A^{(M)}$ 15

Capitolo 2. Anelli noetheriani e teorema di Hilbert 17

Capitolo 3. Estensioni di campi 21
3.1. Estensioni semplici di campi 21
3.2. Estensione di campi come spazio vettoriale. Grado di un'estensione 22
3.3. Campo di spezzamento di un polinomio a coefficienti su un campo 25
3.4. Derivazione formale e radici multiple 29
3.5. Campi finiti 30

CAPITOLO 1

Corpi e campi

Definizione 1.0.1. Si dice **dominio (d'integrità)** un anello commutativo senza divisori dello zero.

Osservazione 1.0.1. Ricordiamo che in un dominio a fattorizzazione unica (UFD) esiste sempre l'MCD tra due elementi non nulli.

Definizione 1.0.2. Definiamo **corpo** un anello in cui ogni elemento non nullo è unitario, ovvero è invertibile rispetto al prodotto. Si dice **campo** un corpo commutativo.

Alternativamente, si può definire un corpo un anello nel quale le seguenti equazioni hanno una sola soluzione:

$$\begin{cases} ax = b & a \neq 0 \\ ya = b \end{cases}$$

Lemma 1.0.1. *Ogni sottoanello di un campo è un dominio. Ogni dominio è immergibile in un campo.*

Teorema 1.0.1. *Sia D un dominio. Allora esiste un campo $F \subseteq D$ isomorfo a D come sottoanello.*

Dimostrazione. Vogliamo costruire il più piccolo campo che contiene D come sottoanello (e per tanto isomorfo a D).

Supponiamo che D sia contenuto come sottoanello in un campo E. Chiamiamo F l'intersezione di tutti i sottocampi di E che contengono D (sottocampo di E generato da D).

Dico che

$$F = \{ab^{-1} | a, b \in D, b \neq 0\}$$

Ovviamente F è un sottoinsieme di E, infatti:

$$\begin{aligned} ab^{\cdot 1} - cd^{-1} &= ab^{\cdot 1}dd^{-1} - cd^{-1}bb^{-1} = (ad - bc)(bd)^{-1} \in F \\ c &\neq 0 \\ (ab^{-1})(cd^{-1})^{-1} &= ad(bc)^{-1} \in F \end{aligned}$$

Ogni sottocampo di E contenente D contiene necessariamente ogni elemento della forma ab^{-1}(con $a, b \in D, b \neq 0$), quindi F è il più piccolo sottocampo di E contenente D. □

Nota 1.0.1. Se D è un anello non commutativo, allora non è sempre vero che possa essere contenuto come sottoanello in un campo.

Sia D un dominio arbitrario. Vogliamo costruire un campo che contenga come sottoanello $D^* = D \setminus \{0\}$; Sia $D \times D^* = \{(a,b) | a \in D, b \in D^*\}$ il prodotto cartesiano di D e D^*.

In $D \times D^*$ definiamo la seguente relazione:

$$(a,b) \sim (c,d) \Leftrightarrow ad = cb$$

$\sim$ è una relazione di equivalenza. Passiamo dunque all'insieme quoziente rispetto a $\sim$: $D \times D^* / \sim$. Denotiamo con il simbolo $\frac{a}{b}$ la classe di equivalenza $[(a,b)]_\sim$contenente la coppia (a,b). Chiamiamo frazione $(\frac{a}{b})$ quella che propriamente sarebbe una classe di equivalenza.

Sia $F = D \times D^* / \sim = \{\frac{a}{b}\} = \{$insieme di tutte le frazioni$\}$. In F definisco ora delle operazioni:

- somma: $\frac{a}{b} + \frac{c}{d} = \frac{ad+cb}{bd}$;
- prodotto: $\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$;

Entrambe le operazioni sono ben definite su F e commutative in quanto D commutativo. Queste due operazioni danno ad F la struttura di un campo:

(1) $(F,+)$ gruppo abeliano additivo (zero : $\frac{0}{1}$);
(2) $(F,\cdot)$ gruppo abeliano moltiplicativo (unità: $\frac{1}{1}$).
    Per verificare che è un gruppo moltiplicativo considero $\frac{a}{b} \in F \Leftrightarrow a \neq 0$, infatti ogni elemento non nullo deve essere invertibile rispetto al prodotto: $(\frac{a}{b})^{-1} = \frac{b}{a}$.
(3) Valgono le proprietà distributive.

Consideriamo ora l'applicazione $\eta_D : D \to F$ tale che $a \mapsto \frac{a}{1}$. Risulta immediato verificare che:

- $\eta_D(a+b) = \frac{a+b}{1} = \frac{a}{1} + \frac{b}{1}$;
- $\eta_D(a \cdot b) = \frac{ab}{1} = \frac{a}{1} \cdot \frac{b}{1}$;
- $\eta_D(1_D) = \frac{1_D}{1} = 1_F$;

Inoltre $\ker \eta_D = 0$, infatti $\frac{a}{1} = 0_F = \frac{0}{1}$. Allora $a \cdot 1 = 1 \cdot 0 = 0 \Rightarrow a = 0$.

Allora η_Dè un monomorfismo di anelli. In particolare $D \simeq \eta_D(D)$, si può quindi identificare D con $\eta_D(D)$ e considerare D come un sottoanello di F.

Osserviamo inoltre che $\forall \frac{a}{b} \in F : \frac{a}{b} = \frac{a}{1} \cdot (\frac{b}{1})^{-1} \simeq ab^{-1}$.

Si conclude che D genera F, cioè che l'unico sottocampo di F contenente D è F stesso.

Definizione 1.0.3. Diremo che F è il **campo dei quozienti** (o *campo delle frazioni*) del dominio D.

Teorema 1.0.2. *Siano D,F rispettivamente un dominio ed un campo, definiti come sopra. Sia $\eta_D : D \to F'$ un monomorfismo di D in un campo F', con F' un altro campo in cui è immergibile D. Allora η_D si estende in un unico modo ad un morfismo $\eta_F : F \to F'$.*

Dimostrazione. Dobbiamo dimostrare unicità ed esistenza del monomorfismo η_F.

- unicità: $\forall a \in D$ poniamo $\eta_D(a) = a'$ (per semplificare la notazione). Dato che ogni elemento di F è scrivibile nella forma: $ab^{\cdot 1} : a, b \in D\ b \neq 0$ allora η_F è completamente determinato dalla relazione precedente. Quindi η_F è unico.

– esistenza:

(Dato che esiste è unico, dobbiamo solo dimostrare che $ab^{-1} = a'(b')^{-1}$, che è un monomorfismo e che è ben definito). Definiamo $\eta_F : ab^{\cdot 1} \to a'(b')^{-1}$. Allora:

– η_F è ben definita:

$$\begin{aligned} ab^{-1} &= cd^{-1} \Rightarrow ad = cb \\ a'd' &= b'c' \text{ poichè } \eta_D \text{ conserva il prodotto} \\ a'(b')^{-1} &= c'(d')^{-1} \end{aligned}$$

– η_F è un morfismo poichè conserva somma e prodotto.

Allora η_F estende η_D, in particolare: $\eta_F(1_F) = \eta_F(1_D) = 1_{F'}$.

Si conclude che η_F è un morfismo di campi non banale che estende η_D, dunque: $\ker \eta_F = 0$, cioè η_F è un monomorfismo.

□

Nota 1.0.2. Notiamo che:

– se $F' = \eta_D(D)$ allora $F' \simeq F$;
– questo teorema esprime in termini alternativi la minimalità di F, utilizzando i campi quoziente.

Esempio 1.0.1.

(1) $D = \mathbb{Z}$ e $F = \mathbb{Q}$.
(2) Sia $D = \mathbb{K}[x]$. Allora $F = \mathbb{K}[x]$ è il campo delle funzioni razionali a coefficienti in $\mathbb{K}$, cioè data $g(x) \neq 0$ si ha che:

$$\frac{f(x)}{g(x)} = f(x) \cdot g(x)^{-1} \in \mathbb{K}[x]$$

Definizione 1.0.4. Sia A un anello con 1_A unità dell'anello e sia $X \subseteq A$ t. c. $X \neq \emptyset$. $\langle X \rangle$ denota il *sottoanello generato dall'insieme X*, cioè per definizione l'intersezione di tutti i sottoanelli che contengno X. Si dice **sottoanello primo** (o minimo) di A il sottoanello generato dall'unità 1_A.

Proposizione 1.0.1. *Il sottoanello primo* $\langle 1_A \rangle$ *di A è* $\mathbb{Z}_{1_A} = \{z \cdot 1_A | \forall z \in \mathbb{Z}\} = \{$*insieme di tutti i multipli dell'unità*$\}$.

Dimostrazione.

– $\mathbb{Z}_{1_A}$è un anello;
– ogni sottoanello di A che contiene 1_A contiene anche $\mathbb{Z}_{1_A}$ (poichè chiuso rispetto alla somma).

□

Dato $\varphi : \mathbb{Z} \to \mathbb{Z}_{1_A}$ l'epimorfismo di anelli tale che $z \mapsto z \cdot 1_A$, ci sono due possibilità: se $\ker \varphi = \{0\} \Rightarrow \mathbb{Z}_{1_A} \simeq \mathbb{Z}$, altrimenti $\ker \varphi \neq \{0\} \Rightarrow \ker \varphi$ è un ideale principale generabile dal minimo intero contenuto in esso: $\ker \varphi = (n) = n\mathbb{Z} \Rightarrow \mathbb{Z}_{1_A} \simeq \frac{\mathbb{Z}}{n\mathbb{Z}}$. In particolare, se $\ker \varphi = (n) \neq 0$ e A è privo di divisori dello zero, allora $(n) = p$ con p primo.

Definizione 1.0.5. Se $\ker \varphi = \{0\}$, si dice che A ha caratteristica 0 (carA). Se $\ker \varphi = (n) \neq \{0\}$ allora si dice che l'anello ha caratteristica n (car n).

Questo vale in particolare se A è un campo. I campi si dividono in :

- campi di caratteristica 0;
- campi di caratteristica $(n) = p$ con p numero primo.

Definizione 1.0.6. Sia F un campo. Si dice sottocampo generato da un sottoinsieme $X \neq \varnothing$ di F, l'intersezione di tutti i sottocampi che contengono X. L'intersezione di tutti i sottocampi di F, denotato con F_0, si dirà **sottocampo primo** di F o **sottocampo minimo** di F.

Poichè F è un campo, esso avrà un sottoanello primo.

Osserviamo che il sottoanello primo di F può essere:

- isomorfo a $\mathbb{Z}$;
- isomorfo a $\mathbb{Z}/p\mathbb{Z}$, campo delle classi di resto modulo p.

Lemma 1.0.2. *Sia F_0 il sottocampo primo di F. Ci sono due casi:*

1. *se $carF = p > 0$, allora $F_0 \simeq \frac{\mathbb{Z}}{p\mathbb{Z}}$;*
2. *se $carF = 0$, allora $F_0 \simeq \mathbb{Q}$.*

Dimostrazione.

1. il sottocampo primo è isomorfo a $\frac{\mathbb{Z}}{p\mathbb{Z}}$, quindi è un campo , quindi è anche il sottocampo primo.
2. $\mathbb{Z}_{1_A} \simeq \mathbb{Z}$. Per il teorema (1.0.2)esiste un monomorfismo dal campo delle frazioni di $\mathbb{Z}$ in F, ovvero un monomorfismo di $\mathbb{Q}$ in F. Per le proprietà di minimalità del campo dei quozienti, il sottocampo primo di F è isomorfo a $\mathbb{Q}$.

□

1.1. Estensioni polinomiali di UFD

Sia D un dominio a fattorizzazione unica (UFD) e sia $D[x]$ il corrispondente anello di polinomi in x. Chiaramente anche $D[x]$ è un dominio.

Lemma 1.1.1. *Se D è UFD, allora $D[x]$ è UFD.*

Sia $f(x) = 0$ un polinomio in $D[x]$ (a coefficienti di D). Sia c l'MCD tra i coefficienti i $f(x)$. Allora c è unico a meno di elementi unitari di D.

Definizione 1.1.1. Diremo che $f(x)$ è primitivo se $c \sim 1_D$ (c è associato a 1_D).

Nota 1.1.1. Sia $f(x) = a_n x^n + \ldots + a_1 x + a_0 \in D[x]$. Per ogni i sia $a_i = c \cdot a_i'$ ($c|a_i$ poichè è $c = MDC_i(a_i)$) e quindi $f(x) = c \cdot f_1(x)$ ove $f_1(x)$ è primitivo

Se $f(x) = c_1 \cdot f_2(x)$ ove $c_1 \in D$ e $f_2(x) \in D[x]$ primitivo, allora posta $f_2(x) = a_n'' x^n + \ldots + a_1'' x + a_0''$ sarà $a_i = c_1 a_i''$ $\forall i$. Chiaramente sarà $c_1 \sim c$, da cui anche $f_1(x) \sim f_2(x)$.

Lemma 1.1.2. *Sia $f(x) \neq 0$ in $F[x]$, con F campo delle frazioni di F. Allora posso scrivere $f(x)$ nella forma $f(x) = \alpha \cdot f_1(x)$. Tale fattorizzazione è unica a meno di elementi unitari di D.*

Dimostrazione. Sia $f(x) = \sum_0^n \alpha_i x^i \in F[x]$ (e $\alpha_n \neq 0$). Allora $\alpha_i = a_i b_i^{-1}$ con $a_i, b_i \in D$ $\forall i$. Poniamo $b = \prod_0^n b_i$. Ovviamente $b \cdot f(x) \in D[x]$ e dunque $bf(x) = cf_1(x)$. Dato c l'MCD dei coefficienti di $bf(x)$ in D e $f_1(x)$ primitivo in $D[x]$ e posto $\alpha = cb^{-1} \in F$, segue che $f(x) = \alpha f_1(x)$ come nella tesi.

Dimostriamo ora l'unicità. Sia $f(x) = \beta f_2(x)$ con $\beta \in F$ e $f_2(x)$ primitivo in $D[x]$. Dato $\beta = d \cdot e^{-1}$ con $e, d \in F$ si ha che $f(x) = cb^{-1} f_1(x) = de^{-1} f_2(x)$. Da qui otteniamo:

$$cef_1(x) = dbf_2(x) \in D[x]$$

Dato che $bd, ce \in D$, allora per la nota (1.1.1) $ce \sim bd$, cioè $uce = bd$ con $u \in D^*$ elemento unitario di D. Allora $\beta = de^{-1} = ucb^{-1} = u\alpha$, cioè $\beta \sim \alpha$, allora $\alpha f_1(x) = \beta f_2(x) = (u\alpha) f_2(x) = \alpha(u f_2(x))$, cioè $f_1(x) \sim f_2(x)$. □

Corollario 1.1.1. *Siano $f(x)$ e $g(x) \in D[x]$ primitivi e associati in $F[x]$. Allora $f(x)$ e $g(x)$ sono associati in $D[x]$.*

Dimostrazione. Per ipotesi $1 \cdot f(x) = \alpha g(x)$ con $\alpha \in F, \alpha \neq 0$. Per il lemma (1.1.2)si ha che $\alpha \sim 1$, cioè $\alpha = u \cdot 1$ con u elemento unitario di D. Allora $u = \alpha \in D$ e pertanto $f(x) = u \cdot g(x)$, cioè $f(x) \sim g(x)$ in $D[x]$. □

Lemma 1.1.3. **(generale)***: Siano A,B anelli. Sia $\varphi\colon A \to B$ un morfismo di anelli. Allora φ si estende ad un morfismo di anelli $\tilde{\varphi}\colon A[x] \to B[x]$ tale che*

$$f(x) = \sum_0^n a_i x^i \mapsto \tilde{\varphi}[f(x)] = \sum_0^n \varphi(a_i) x^i$$

Lemma 1.1.4. **(di Gauss):** *Il prodotto di due polinomi primitivi $f(x), g(x) \in D[x]$ è un polinomio primitivo $f(x) \cdot g(x) \in D[x]$.*

Dimostrazione. Per assurdo supponiamo che $h(x) = f(x) \cdot g(x)$ non sia primitivo. Allora l'MCD dei coefficienti di $h(x)$ non è unitario. Pertanto, essendo D un UFD, ha un'unica fattorizzazione in irriducibili. Esiste, dunque, un elemento irriducibile tale che divida tutti i coefficienti di h(x) ma che non divida i coefficienti di $f(x)$ e di $g(x)$ in quanto primitivi. In altre parole:

$$\exists p \text{ irriducibile t.c. } p \mid h(x) \text{ ma } p \nmid f(x) \ \wedge \ p \nmid g(x)$$

Dato che D è UFD, allora p è anche primo in D $\Rightarrow \tilde{D} = \frac{D}{(p)}$ è un dominio. Consideriamo ora l'epimorfismo canonico $\varphi\colon D \to \tilde{D}$ e la sua estensione agli anelli di polinomi $\tilde{\varphi}\colon D[x] \to \tilde{D}[x]$. Essendo $\tilde{D}$ un dominio, anche $\tilde{D}[x]$ è un dominio e per tanto

$$0 = \tilde{\varphi}[h(x)] = \tilde{\varphi}[f(x) \cdot g(x)] = \tilde{\varphi}[f(x)] \cdot \tilde{\varphi}[g(x)]$$

Essendo $\tilde{\varphi}[h(x)]$ il polinomio $h(x)$ con tutti i coefficienti scritti in modulo p, allora $\tilde{\varphi}[h(x)] = 0$ poichè $p \mid h(x)$ e quindi anche tutti i coefficienti. Ma per definizione $\tilde{\varphi}[f(x)] \neq 0 \ \wedge \tilde{\varphi}[g(x)] \neq 0$ ed essendo D un dominio, allora $\tilde{\varphi}[f(x)] \cdot \tilde{\varphi}[g(x)] \neq 0$. Contraddizione. Vale la tesi. □

Lemma 1.1.5. *Sia $f(x) \in D[x]$* [1]*. Sia $f(x)$ irriducibile di $\deg f(x) > 0 \Rightarrow f(x)$ irriducibile in $F[x]$, ove F è il campo delle frazioni di D.*

Dimostrazione. $f(x)$ è sicuramente primitivo [2] . Supponiamo, per assurdo, $f(x)$ riducile in $F[x]$, allora $f(x) = a(x) \cdot b(x)$ con $a(x), b(x) \in F[x]$ entrambi con $\deg > 0$. Per il lemma (1.1.2) si può scrivere $a(x) = \alpha f_1(x)$ e $b(x) = \beta f_2(x)$

[1] D è un UFD

[2] in caso contrario posso considerare $f(x) = a \cdot \bar{f}(x))$ con $a \in D$, a non unitario e non associato a $f(x)$. Allora $a \cdot \bar{f}(x)$ è una fattorizzazione non banale in irriducibili, quindi $f(x)$ sarebbe riducibile in $D[x]$.

con $\alpha, \beta \in F$ e $f(x)$ e $g(x)$ primitivi in $D[x]$. Allora $f(x) = \alpha\beta f_1(x)f_2(x)$ ove per il lemma (1.1.4) di Gauss, $f_1(x)f_2(x)$ è primitivo in $D[x]$. Segue, per il corollario (1.1.1)che $f(x)$ e $f_1(x)f_2(x)$ differiscono per un elemento unitario. Poichè $\deg f_i(x) > 0$ per $i = 1, 2$, si contraddice l'irriducibilità di $f(x)$ in $D[x]$. Assurdo. Vale la tesi. □

Teorema 1.1.1. *Se D è un UFD, tale è anche $D[x]$.*

Dimostrazione. Sia $0 \neq f(x) \in D[x]$, con $f(x)$ non unitario.

(1) *Esistenza della fattorizzazione.* Sia $f(x) = d \cdot f_1(x)$ ove $d \in D$ e $f_1(x) \in D[x]$ primitivo. Se d non fosse unitario, esisterebbero alcuni d_i tali che $d = d_1 \cdot d_2 \cdot \ldots \cdot d_r$ con i d_i irriducibili in D (e in $D[x]$ di conseguenza). Consideriamo $f_1(x)$. Si può ovviamente supporre che $\deg f_1(x) > 0$ (altrimenti sarebbe $f_1(x) \sim 1$ e sarebbe conclusa la dimostrazione). Se $f_1(x)$ irriducibile, allora abbiamo fattorizzato $f(x)$. Se così non fosse, potremmo scomposse in:

$$f_1(x) = f_2(x) \cdot f_3(x)$$

con $\deg f_2(x)$, $\deg f_3(x) < \deg f_1(x)$ e $f_2(x), f_3(x)$ sono primitivi, altrimenti $f_1(x)$ non sarebbe primitivo. Per induzione sul grado, gli f_i sono fattorizzabili e si conclude che $f_1(x) = q_1(x) \cdots q_s(x)$ con i $q_j(x)$ irriducibili in $D[x]$.

(2) *Unicità (a meno di fattori unitari).* Si può distinguere in due casi: -1
   (a) Supponiamo $f(x)$ primitivo. Allora ogni sua fattorizzazione $f_1(x) = q_1(x) \cdots q_s(x)$ in irriducibili in $D[x]$, tutti i suoi fattori $q_j(x)$ sono primitivi e con $\deg q_j(x) > 0$ [3]. Sia ora $f_1(x) = p_1(x) \cdots p_t(x)$ un'altra fattorizzazione. Allora per il lemma (1.1.4)i polinomi p_j e q_i sono tutti associati : $p_i(x) \sim q_i(x)$ a meno di un riordinamento in $F[x]$. Per il corollario (1.1.1)si ha che $p_i(x) \sim q_i(x)$ in $D[x]$.
   (b) Siaa $f(x)$ non primitivo. I fattori irriducibili di grado positivo sono primitivi, quindi il loro prodotto è primitivo per il lemma (1.1.4). Ne segue che ogni fattorizzazione di $f(x)$ in irriducibili in $D[x]$ il prodotto dei fattori di grado nullo deve essere necessariamente un MCD dei coefficienti non nulli di $f(x)$. In altre parole, se

$$f(x) = d_1 \cdot \textstyle\prod_j f_j(x) \quad = d_2 \cdot \prod_i g_i(x)$$

sono due fattorizzazioni tali che, a meno di elementi unitari si possa supporre $d_1 = d_2$ e essendo $d_i \in D$ hanno un unica fattorizzazione. Sia, in ultimo,

$$\prod_i g_i(x) = \prod_j f_j(x)$$

è primitivo e si torna duqnue al caso precedente.

□

[3]Altrimenti $f(x)$ non sarebbe primitivo, infatti se $\deg q_j(x) = 0$, allora q_j sarebbe una costante in D.

1.2. Polinomi in più variabili

Esistono diversi modi per costruire un anello di polinomi in più variabili.

- Sia A un anello commutativo e siano $x_1, x_2, \ldots, x_n$ delle indeterminate (variabili). Allora l'anello$A[x_1, x_2, \ldots, x_n] = (A[x_1, \ldots, x_{n-1}])[x_n]$ è definito intuitivamente come l'anello nell'indeterminata x_n a coefficienti in $A[x_1, \ldots, x_{n-1}]$. Per $n = 1$ si intende $A[x_1, \ldots, x_n] = A$.
- Costruzione generale (alternativa).

  NOTA 1.2.1. Se una proprietà si eredita $A \to A[x]$ si ereda anche ad $A \to A[x_1, \ldots, x_n]$ per successivi trasporti.

  Sia A un anello commutativo e sia $(M, +)$ un monoide commutativo. Consideriamo l'insieme $A^{(M)}$ di tutte le funzioni $f\colon M \to A$ quasi ovunque nulle [4] Ogni funzione così fatta si può esprimere come una famiglia $(a_\mu)_{\mu\in M}$ ove $a_\mu = f(\mu)$ e $a_\mu = 0_A$ quasi ovunque.

  Si può dare ad $A^{(M)}$ la struttura di anello commutativo ponendo:
  - $(a_\mu)_{\mu\in M} + (b_\mu)_{\mu\in M} = (a_\mu + b_\mu)_{\mu\in M}$;
  - $(a_\mu)_{\mu\in M} \cdot (b_\mu)_{\mu\in M} = (c_\mu)_{\mu\in M}$ con $c_\mu = \sum_{\lambda+\nu=\mu} a_\lambda b_\nu$ per $\lambda, \nu, \mu \in M$.

ESEMPIO 1.2.1. Sia $M = \mathbb{N}_0$ e $f \in A^{(\mathbb{N}_0)}$. Le funzioni saranno della forma: $f = \sum_0^m a_i x^i$ con $a_i = a_\mu$.

Nel caso di M generico, possiamo ancora dare una scrittura polinomiale per gli elementi dell'anello $A^{(M)}$. Precisamente per ogni $\mu \in M$ fissato, poniamo

$$X^\mu := (\delta_{\mu,\lambda})_{\lambda\in M} \quad \text{con } \delta_{\mu,\lambda} \text{ delta di Kronecker}$$

la funzione da M in A cha vale 1_A su μ e 0_A su $\lambda \neq \mu$.

DEFINIZIONE 1.2.1. Diremo che X^μ è il **monomio (standard) di tipo** μ.

Allora si vede subito che l'elemento $(a_\mu)_{\mu\in M}$ si scrive in uno e un solo modo nella forma[5]:

$$f = \sum_{\mu\in M} a_\mu X^\mu.$$

Valgono le seguenti operazioni:

- somma:

$$\sum_{\mu\in M} a_\mu X^\mu + \sum_{\mu\in M} b_\mu X^\mu = \sum_{\mu\in M} (a_\mu + b_\mu) X^\mu$$

- prodotto:

$$(\sum_{\mu\in M} a_\mu X^\mu)(\sum_{\mu\in M} b_\mu X^\mu) = \sum_{\mu\in M} (\sum_{\lambda+\nu=\mu} a_\lambda b_\nu) X^\mu \text{ con } \lambda, \nu \in M$$

NOTA 1.2.2. Il polinomio nullo: $a_\mu = 0\ \forall \mu \in M$ è lo zero di $A^{(M)}$. X^0 è l'unità di $A^{(M)}$ ed esiste il monomorfismo che immerge A in $A^{(M)}$:

$$A \hookrightarrow A^{(M)} \quad \forall a \in A \quad a \mapsto aX^0$$

[4] nulle ovunque tranne che per un numero finito di elementi di M.

[5] Si tratta della funzione caratteristica. La somma nella scrittura di f è una somma finita.

1.3. Radici di polinomi

Sia D un dominio a fattorizzazione unica e F il campo delle frazioni di D. Allora gli elementi di $F[x]$ sono della forma:

$$f(x) = \sum_{i=0}^{n} a_i X^i \in F[x] \quad \text{con } a_n \neq 0$$

Voglio cercare le radici di questo polinomio $f(x)$. Ci sono vari criteri:

(1) Si può supporre sempre che $f(x) \in D[x]$, perchè si può moltiplicare $f(x)$ per l'm.c.m. dei denominatori.

Criterio 1.3.1. *Sia D un UFD, e F il campo delle frazioni di D. Allora le eventuali soluzioni di $f(x) \in D[x]$ hanno la forma $q = \frac{r}{s}$ con $r \mid a_0\,, s \mid a_n$.*

Dimostrazione. Supponiamo $f(q) = 0$ con $q = \frac{r}{s} \in F$ e $MCD(r, s) = 1$. Allora

$$0 = f(q) = a_n \frac{r^n}{s^n} + \ldots + a_1 \frac{r}{s} + a_0$$

Moltiplico per s^n:

$$s^n \cdot 0 = 0 = a_n r^n + a_{n-1} r^{n-1} s + \ldots + a_1 r s^{n-1} + a_0 s^n$$

Questo significa che $s \mid a_n r^n$, infatti possiamo scrivere:

$$a_0 s^n = -(a_n r^n + \ldots + a_1 r s^{n-1})$$

Questo implica che $s \mid a_n$, essendo $MCD(r, s) = 1$. Analogamente si avrà che $r \mid a_0 s^n$, in quanto è possibile riscrivere tutto nella forma:

$$a_n r^n = -(a_{n-1} r^{n-1} s + \ldots + a_0 s^n)$$

Come prima si ha che $r \mid a_0$, poichè $MCD(r, s) = 1$. Dunque la tesi. □

Esempio 1.3.1. Facciamo alcuni esempi di applicazione per il criterio (1.3.1):

(1) $f(x) = 4x^3 + 6x^2 - 27$. Le possibili soluzioni sono: per il numeratore $\{\pm 1, \pm 3, \pm 9, \pm 27\}$ e per il denominatore $\{\pm 1, \pm 2, \pm 4\}$. Con denominatore ± 1 non esistono soluzioni. Riscriviamo il polinomio nella forma

$$f(x) = x^3 + \frac{3}{2}x^2 - \frac{27}{4}$$

e vediamo che usando il criterio (1.3.1)troviamo la soluzione: $+\frac{3}{2}$.

(2) Sia $x^5 - 15 \in \mathbb{Q}[x]$. Irriducibile.

Nota 1.3.1. In generale, se si ha $x^n - a$, con a che non è un quadrato perfetto, allora $x^n - a$ è irriducibile.

(3) $f(x) = x^3 + 3x^2 - 4x - 1 \in \mathbb{Z}[x]$. Considero il morfismo $\Phi : \mathbb{Z} \to \frac{\mathbb{Z}}{3\mathbb{Z}}[x]$. Allora $\Phi(f(x)) = x^3 - x - 1 = x^3 + 2x - 2$. Vediamo che in $\frac{\mathbb{Z}}{3\mathbb{Z}}$ $\Phi(f(x))$ non ammette soluzioni. Allora è irriducibile in $\frac{\mathbb{Z}}{3\mathbb{Z}}$, quindi anche in $\mathbb{Q}$ e quindi anche in $\mathbb{Z}$.

Criterio 1.3.2. *(di Eisentein): Sia D un UFD e sia $f(x) = \sum_0^n a_i x^i \in D[x]$ un polinomio di* deg $f(x) = n > 0$ *e primitivo in $D[x]$. Se esiste un primo $p \in D$, tale che $p \nmid a_n$ ma $p \mid a_i\ \forall i = 0, \ldots, n-1$ e $p^2 \nmid a_0$, allora $f(x)$ è irriducibile in $D[x]$ e quindi in $F[x]$.*

DIMOSTRAZIONE. Per assurdo, sia $f(x) = g(x) \cdot h(x) \in D[x]$ con $g(x) = \sum_0^r b_i x^i$ e $h(x) = \sum_0^s c_j x^j$ in modo tale che $r + s = n$ e $r, s > 0$.

Moltiplichiamo $g(x) \cdot h(x)$. Segue che :

$$\begin{aligned} a_n &= b_r c_s \neq 0 \quad \text{per ipotesi} \\ a_0 &= b_0 c_0 \end{aligned}$$

Sempre per ipotesi deve essere che

$$\begin{array}{ccccc} p \nmid a_n & \Rightarrow & p \nmid b_r & \wedge & p \nmid c_s \\ p \mid a_i & \Rightarrow & p \mid b_i & \vee & p \mid c_i \\ p^2 \nmid a_0 & \Rightarrow & p \mid b_0 & \dot{\vee} & p \mid c_0 \end{array}$$

Supponiamo quindi che $p \mid b_0 \wedge p \nmid c_0$ e sia $t \leq r$ il massimo indice tale per cui $p \mid b_k \quad \forall 0 \leq k \leq t$. Posto $b_i = 0 \; \forall i > r$ e $c_j = 0 \; \forall j > r$, risulta che

$$a_{t+1} = b_0 c_{t+1} + b_1 c_t + \ldots + b_t c_1 + b_{t+1} c_0$$

con $p \mid b_0 c_{t+1}, b_1 c_t, \ldots, b_t c_1$ ma $p \nmid b_{t+1} c_0$. . Allora $p \nmid a_{t+1} \Rightarrow n = t + 1$ (per le ipotesi), allora $r = n$ e $s = 0$, assurdo perchè $s > 0$ per ipotesi. □

CRITERIO 1.3.3. *(di Riduzione modulo p) Sia D un UFD e sia $p \in D[x]$ primo e $0 \neq f(x) \in D[x]$ con $f(x) = \sum_0^n a_i x^i$ con $a_n \neq 0$ e $p \nmid a_n$. Sia $\Phi \colon D[x] \to \frac{D}{(p)}[x]$ l'omomorfismo canonico che riduce i coefficienti in modulo p[6]. Se $\Phi(f(x))$ è irriducibile in $\frac{D}{(p)}[x]$, allora $f(x)$ è irriducibile in $F[x]$. Se inoltre $f(x)$ è primitivo, allora $f(x)$ irriducibile in $D[x]$.*

DIMOSTRAZIONE. Assumiamo $f(x)$ primitivo. Se $f(x)$ riducibile, allora $f(x) = h(x)g(x) \in D[x]$ con $g(x) = \sum_0^r b_i x^i$ e $h(x) = \sum_0^s c_j x^j$ con $c_s, b_r \neq 0$ e $r, s > 0$.

Per ipotesi deve essere $p \nmid a_n \Rightarrow p \mid b_r \vee p \mid c_s$. Allora $\Phi(f(x)) = \Phi(h(x))\Phi(g(x))$ con $\Phi(h(x)), \Phi(g(x))$ non costanti poichè $p \nmid b_r, c_s$. Allora $\Phi(f(x))$ è riducibile in $\frac{D}{(p)}[x]$, ma questo contraddice l'ipotesi. Allora $f(x)$ irriducibile in $D[x]$ e per tanto ance in $F[x]$.

Se $f(x)$ non è primitivo allora posso scomporre il polinomio in $f(x) = c \cdot \tilde{f}(x)$ con $\tilde{f}(x)$ primitivo in $D[x]$. Allora $p \nmid c$ e $p \nmid \tilde{a}_n$ con $\tilde{a}_n$ coefficiente direttivo di $\tilde{f}(x)$. Per ipotesi $\Phi(f(x))$ è irriducile, quindi $\Phi(\tilde{f}(x))$ è irriducibile in $\frac{D}{(p)}[x]$, allora $\tilde{f}(x)$ irriducibile in $D[x]$ per il punto precedente e per tanto $\tilde{f}(x)$ irriducibile in $F[x]$. F è un campo quindi gli associati di un polinomio irriducibile sono irriducibili. Allora $f(x)$ è irriducibile in $F[x]$. □

Consideriamo $M = \mathbb{N}_0^n$ e siano $\mu = (\mu_1, \ldots, \mu_n)$ gli elementi di questo campo. Poniamo $\forall 1 \leq i \leq n \; x_i = X^{(0,\ldots,1,\ldots,0)}$ con 1 al posto i-esimo. Per la definizione di prodotto di polinomi si vede subito che

$$X^\mu = (x_1^{\mu_1}, \ldots, x_n^{\mu_n})$$

e ogni $f \in A^{(M)}$ si scrive in modo unico come:

$$f = \sum_\mu a_{\mu_1,\ldots,\mu_n} x_1^{\mu_1} \cdots x_n^{\mu_n}$$

6

DEFINIZIONE 1.3.1. Chiamiamo il morfismo Φ **riduzione modulo p**.

si tratta di una somma finita, poichè la maggior parte degli $a_{\mu_1,\ldots,\mu_n}$ sono nulli.

Invece di $A^{(M)}$ scriveremo $A[x_1,\ldots,x_n]$ o anche $A[X]$ intendendo con $X = (x_1,\ldots,x_n)$ il sistema delle indeterminate x_i.

OSSERVAZIONE 1.3.1. Osserviamo che $A[x_1,\ldots x_n]$ è canonicamente isomorfo all'anello. Allora $A[x_1,\ldots,x_{n-1}][x_n]$ sarà l'anello dei polinomi di variabile x_n a coefficienti in $A[x_1,\ldots,x_{n-1}]$.

Per $n = 1$ è possibile identificare $A[x_1,\ldots,x_n]$ con l'anello A.

COROLLARIO 1.3.1. *Sia D un dominio, allora anche $D[x_1,\ldots,x_n]$ è un dominio.*

DIMOSTRAZIONE. L'asserto è vero per $n = 1$. Dimostriamo per induzione: sia vero per n ed essendo

$$D[x_1,\ldots,x_{n+1}] \simeq D[x_1,\ldots,x_n][x_{n+1}]$$

allora vale la tesi. □

DEFINIZIONE 1.3.2. Sia $f = \sum_\mu a_\mu x^\mu \in A[x_1,\ldots,x_n]$. $\forall \mu = (\mu_1,\ldots,\mu_n)$ poniamo $|\mu| = \mu_1 + \ldots + \mu_n$ e scriviamo $\forall i \geq 0$

$$f_i = \sum_{|\mu|=i} a_\mu x^\mu.$$

Diremo che f_i è una componente omogeneo di F avente grado i. Chiaramente il polinomio $f = \sum_{i=0}^{\infty} f_i$ si dice omogeneo di grado i se $f = f_i$ per qualche $i \neq 0$. Se $f \neq 0$, i è univocamente determinata da *f*.

Definiamo il grado complessivo di un polinomio nel modo seguente:

- se $f \neq 0$ si ha che $\deg f = \max\{i \in \mathbb{N}_0 | f_i \neq 0\}$;
- se $f = 0$ si pone $\deg f = -1 \quad \vee \quad \deg f = -\infty$.

LEMMA 1.3.1. *Siano $f, g \in A[x_1,\ldots,x_n]$. Allora:*

(1) $\deg(f+g) \leq \max\{\deg f, \deg g\}$*;*
(2) $\deg(f \cdot g) \leq \deg f + \deg g$. *Vale l'uguaglianza se A è un dominio.*

DIMOSTRAZIONE. Se $f = 0 \ \vee \ g = 0$, allora (1) e (2) banalmente vere.

Siano dunque $f, g \neq 0$ e scriviamo $f = \sum_i f_i$ e $g = \sum_j g_j$ con f_i, g_j componenti omogenee. Allora:

(1) ovvio, poichè $f + g = \sum_i f_i + \sum_j g_j$ e per tanto $\deg(f+g) = \max\{i, j \mid f_i \neq 0 \wedge g_j \neq 0\}$.
(2) Siano $\deg f = s$ e $\deg g = t$. Allora

$f \cdot g = f_s \cdot g_t +$ {somma di componenti omogenee di grado inferiore}

. Allora $\deg(f \cdot g) \leq s+t$. Se A è un dominio, allora $A[x_1,\ldots,x_n]$ dominio e quindi $f_s g_t \neq 0$, poichè f_se g_t sono non nulli per ipotesi e $A[x_1,\ldots,x_n]$ non contiente divisori dello zero. In questo caso, $\deg(f \cdot g) = s + t = \deg f + \deg g$.

In particolare, essendo A un dominio, gli elementi unitari di $A[x_1,\ldots,x_n]$ sono tutti e soli gli elementi unitari di A.

Caso generale: sia I un insieme di indici. Consideriamo il monoide additivo commutativo $M = \mathbb{N}_0^{(I)}$. Per ogni $i \in I$ poniamo $\varepsilon_i \in \mathbb{N}_0^{(I)}$ l'elemento definito da:

$$\varepsilon_i(j) = \delta_{i,j} \quad \forall j \in I$$

Scriveremo $x_i = X^{\varepsilon_i}$ (variabile i-esima). Allora $\forall \mu \in \mathbb{N}_0^{(I)} \quad \mu = (\mu_i)_{i\in I} \in \mathbb{N}_0^{(I)}$ si ha $X^\mu = \prod_{i\in I} x_i^{\mu_i}$[7] □

1.4. Proprietà universale di $A^{(M)}$

Proposizione 1.4.1. *Siano $\varphi\colon A \to A'$ un morfismo di anelli e $\sigma\colon M \to A'$ un morfismo di monoidi* [8]*. Allora esiste ed è unico un morfismo di anelli $\Phi\colon A^{(M)} \to A'$ tale che $\Phi\mid_A = \varphi$ e $\Phi(X^\mu) = \sigma(\mu)$.*

Dimostrazione. Se esiste Φ come sopra, allora

$$\begin{aligned} f &= \sum a_\mu X^\mu \in A^{(M)} = \Phi(\sum a_\mu X^\mu) = \sum \Phi(a_\mu X^\mu) \\ &= \sum \Phi(a_\mu)\Phi(X^\mu) = \sum \varphi(a_\mu)\sigma(\mu) \end{aligned}$$

Quindi Φ è unico.

Se ora consideriamo l'applicazione $\sum a_\mu X^\mu \mapsto \sum \varphi(a_\mu)\sigma(\mu)$, si verifica facilmente che questo è un morfismo di anelli. Naturalmente $\forall a \in A \quad a = aX^0 \mapsto \varphi(a)\sigma(0) = \varphi(a)1_{A'} = \varphi(a)$, con $\sigma(0_M) = 1_{A'}$. Similmente $X^\mu = 1_A X^\mu \mapsto \varphi(1_A)\sigma(\mu) = 1_{A'}\sigma(\mu) = \sigma(\mu)$. □

La proprietà espressa è universale e caratterizza $A^{(M)}$ a meno di isomorfismi nel senso seguente:

Proposizione 1.4.2. *Sia $A \hookrightarrow B$ un'estensione di anelli con A sottoanello di B e sia $i\colon M \to B$ un morfismo di monoidi (considero B come un monoide moltiplicativo). Si supponga che B soddisfi le proprietà descritte nella proposizione* (1.4.1)[9]*. Allora $B \simeq A^{(M)}$.*

Dimostrazione. Per la proprietà universale di $A^{(M)}$, esiste un omomorfismo $\Phi : A^{(M)} \to B$ tale che $\Phi\mid_A = Id_A$ e tale che $\Phi(X^\mu) = i(\mu)$. Per la proprietà universale di B, esiste un omomorfismo di anelli $\Psi : B \to A^{(M)}$ tale che $\Psi\mid_A = Id_A$ e $\Psi \circ i = \Psi(i(\mu)) = X^\mu$. Consideriamo ora la composizione $\Phi\circ\Psi\colon B \to B$ e vediamo che è un morfismo di anelli tale che $\Phi\circ\Psi\mid_A = Id_A$ e $(\Phi\circ\Psi)(i(\mu)) = \Phi(X^\mu) = i(\mu)$. Per l'unicità invocata dalla proprietà universale, deve essere $\Phi \circ \Psi = Id_B$. Lo stesso discorso applicato a $\Psi\circ\Phi\colon A^{(M)} \to A^{(M)}$ e l'unicità invocata dalla proprietà universale di $A^{(M)}$ mostra che $\Psi \circ \Phi = Id_{A^{(M)}}$, dunque Φ realizza un isomorfismo tra $A^{(M)}$ e B. □

Nel caso $M = \mathbb{N}_0^n$, il morfismo $\sigma\colon M \to A'$ della propozione (1.4.1)è univocamente determinato dalle n-uple canoniche $(0,\dots,0,1,0,\dots,0)$ con l'1 al posto i-esimo e $1 \le i \le n$. La proposizione (1.4.1) può essere rienunciata nel seguente modo:

Proposizione 1.4.3. *Sia $\varphi\colon A \to A'$ un omomorfismo di anelli e siano $\mu_1,\dots,\mu_n$ elementi di A'. Allora esiste ed è unico l'omomorfismo di anelli $\Phi : A[x_1,\dots,x_n] \to A'$ tale che $\Phi\mid_A = \varphi$ e $\Phi(x_i) = \mu_i \quad \forall i = 1,\dots,n$.*

Nota 1.4.1. Si ricordi che $x_i = X^{(0,\dots,0,1,0,\dots,0)}$ e il morfismo $\sigma\colon M \to A'$ è tale che: $(0,\dots,0,1,0,\dots,0) \mapsto u_i$.

---

[7] si tratta di un prodotto finito $\forall i$ tranne che per un numero finito $x_i^{\mu_i} = x^0 = 1$.

[8] prendendo A' come monoide rispetto al prodotto

[9] cioè che dati un morfismo di anelli $\psi\colon A \to A'$ e un morfismo di monoidi $\tau\colon M \to A'$, $\exists!$ l'omomorfismo di anelli $\Psi\colon B \to A'$ tale che $\Psi\mid_A = \psi$ e $\Psi \circ i = \tau$.

Posto $U = \{u_1, \dots, u_n\}$ e $U^\mu = u_1^{\mu_1} \cdots u_n^{\mu_n}$ si ha che $\Phi(\sum a_{\mu_1 \dots \mu_n} x_1^{\mu_1} \cdots x_n^{\mu_n}) = \sum \varphi(a_{\mu_1} \dots a_{\mu_n}) u_1^{\mu_1} \cdots u_n^{\mu_n} \in A$ è un polinomio in u_i a coefficienti in A.

Un caso rilevante è quello di un'estensione di anelli. Supponiamo che $\varphi\colon A \to A'$ sia la mappa di inclusione $i\colon A \to A'$, con A sottoanello di A'.

Allora se $f = f(x_1, \dots, x_n) \in A[x_1, \dots, x_n]$, posto $\sum a_{\mu_1 \dots \mu_n} u_1^{\mu_1} \cdots u_n^{\mu_n} = f(u_1, \dots, u_n)$ si avrà che $\Phi(f(x_1, \dots, x_n)) = f(u_1, \dots, u_n)$.

Definizione 1.4.1. Φ si dice **omomorfismo di valutazione** (di un polinomio in n variabili $x_1, \dots, x_n$ a coefficienti in A sulla n-upla $(u_1, \dots, u_n)$ di elementi dell'estensione di A').

Per $\Phi(A[x_1, \dots, x_n])$ scriveremo $A[u_1, \dots, u_n]$ o anche sinteticamente $A[U]$ con $U = \{u_1, \dots, u_n\}$. Chiaramente $A[U]$ è il sottoanello di A' generato dal sottoinsieme $A \cup U$ e consise dell'intersezione di tutti i sottoanelli di A' che contengono A e U.

Definizione 1.4.2. Se $f(u_1, \dots, u_n) = 0_A$, diremo che la n-upla $(u_1, \dots, u_n)$ è uno **zero** del polinomio f.

Definizione 1.4.3. Sia $A \hookrightarrow B$ un'estensione di anelli e $(u_1, \dots, u_n) \in B$. Se l'omomorfismo di valutazione $\Phi\colon A[x_1, \dots, x_n] \to B$ che prolunga l'identità su A e manda x_i in u_i (con $1 \leq i \leq n$) è iniettivo, diremo che l'insieme $\{u_1, \dots, u_n\}$ è **trascendente** (o algebricamente indipendente) su A. In caso contrario diremo che $\{u_1, \dots, u_n\}$ è **algebrico** (o algebricamente dipendente) su A.

Nota 1.4.2. Si noti che $\{u_1, \dots, u_n\}$ è trascendente su A $\iff \ker \Phi = 0 \iff A[x_1, \dots, x_n] \simeq A[u_1, \dots, u_n] \iff (u_1, \dots, u_n)$ non è uno zero di alcun polinomio non nullo di $A[x_1, \dots, x_n]$.

Analogamente, $\{u_1, \dots, u_n\}$ è algebrico su A $\iff$ esiste almeno un polinomio $0 \neq f \in A[x_1, \dots x_n]$ tale che $f(u_1, \dots, u_n) = 0_A$.

Esempio 1.4.1. Dato $\mathbb{Q} \hookrightarrow \mathbb{R}$, due esempi classici sono quello di e trascendente su $\mathbb{Q}$ (Hermite, 1873) e di π trascendente su $\mathbb{Q}$ (Lindemann, 1882).

CAPITOLO 2

Anelli noetheriani e teorema di Hilbert

Ricordiamo che, dato A un anello commutativo, un ideale I di A è generato da un suo sottoinsieme X se I è l'intersezione di tutti gli ideali di A contenenti il sottoinsieme X, e in quel caso si indica con $I = \langle X \rangle$. Allora:

$$I = \{a_1 x^1 + \ldots + a_n x_n \mid n \in \mathbb{N}; x_i \in X; 1 \leq i \leq n \, e \, a_i \in A \; 1 \leq i \leq n\}$$

In particolare, se X è finito, allora I è finitamente generato.

Lemma 2.0.1. *Sia A un anello commutativo. Sono equivalenti le seguenti condizioni:*

(1) *Ogni ideale di A è finitamente generato;*
(2) *Ogni catena strettamente ascendente di ideali di A è finita, ovvero ogni catena ascendente di ideali di A è stazionaria* [1].
(3) *Ogni collezione non vuota $\mathcal{S}$ di ideali di A contiene un elemento massimale, ovvero dato l'ideale I di $\mathcal{S}$ tale che $J \in \mathcal{S}$ e $J \supseteq I$, allora $J = I$*[2].

Dimostrazione. (1)⇒(2)

Sia $I_1 \subset I_2 \subset I_3 \subset \ldots$ una catena strettamente ascendente di ideali di A e sia $N = \bigcup_j I_j$ un ideale finitamente generato di A. Allora possiamo scriverlo nella forma

$$N = \langle x_1, \ldots, x_n \rangle$$

Esisterà un j_0 tale che $x_1, x_2, \ldots, x_n \in I_{j_0}$. Segue che $\langle x_1, \ldots, x_n \rangle \subseteq I_{j_0} \subseteq N = \langle x_1, \ldots, x_n \rangle$. Allora $N \equiv I_{j_0}$ e la catena termina in I_{j_0}.

(2)⇒(3)

Sia $I_0 \in \mathcal{S}$ con $\mathcal{S}$ collezione non vuota. Se I_0 non è massimale in $\mathcal{S}$ allora $\exists I_1 \in \mathcal{S}$ tale che $I_0 \subsetneq I_1$.Se I_1 non è massimale in $\mathcal{S}$, allora $\exists I_2 \in \mathcal{S}$ tale che $I_1 \subsetneq I_2$. La procedura continua e termina ad un numero finito di passi. In caso contrario si avrebbe una catena strettamente ascendente di ideali di A infinita.

(3)⇒(1)

Sia I un ideale di A e sia $a_0 \in I$. Se $\langle a_0 \rangle \neq I$, $\exists a_1 \in I \setminus \langle a_0 \rangle \Rightarrow \langle a_0 \rangle \subset \langle a_0, a_1 \rangle$. Se $\langle a_0, a_1 \rangle \neq I$, $\exists a_2 \in I \setminus \langle a_0, a_1 \rangle \Rightarrow \langle a_0, a_1 \rangle \subset \langle a_0, a_1, a_2 \rangle$. Procedendo induttivamente si crea una catena ascendente di ideali con inclusioni strette. La collezione $\mathcal{S}$ di ideali così ottenuta deve contenere un elemento massimali, sia esso $\langle a_0, a_1, \ldots, a_{n-1} \rangle$. É chiaro allora che $\langle a_0, a_1, \ldots, a_{n-1} \rangle \equiv I$. □

Definizione 2.0.4. Un anello commutativo A che soddisfi una delle condizioni del lemma (2.0.1) si dice **noetheriano**.

[1] Condizione Catenaria Ascendente (CCA)
[2] Condizione di Massimo (CM)

Lemma 2.0.2. *Sia A noetheriano. Allora ogni immagine epimorfa di A è noetheriano.*

Dimostrazione. Sia $\varphi\colon A \to B$ un epimorfismo di anelli e sia $J_1 \subset J_2 \subset ... \subset J_r$ una catena strettamente ascendente di ideali di B. Per ogni r, $I_r = \varphi^{-1}(J_r)$ la preimmagine di J_r in a mediante φ. Allora I_r è un ideale di A e sia crea la catena strettamente ascendente $I_1 \subset I_2 \subset ... \subset I_r$ di ideali di A. Poichè è noetheriano,supponiamo la catena di arresti ad I_m. Poichè per ogni r, $\varphi(I_r) = J_r$, si ottiene che si arresta in $J_m = \varphi(I_m)$. □

Dimostrare per esercizio che ogni dominio ad ideali principali è un dominio noetheriano.

Teorema 2.0.1. ***(della base di Hilbert, 1890):***
Se A è noetheriano, allora anche $A[x]$ noetheriano.

Dimostrazione. Sia $I[x]$ un ideale di $A[x]$ $\forall i \in \mathbb{N}_0$. Definiamo $I_i = \{a \in A \mid \exists f(x) \in I[x]\, t.c.\ f(x) = ax^i + \ldots + a_1x + a_0\}$. Si verifica facilmente che $\forall i$ I_i è un ideale di A. Inoltre $\forall i$ $I_i \subseteq I_{i+1}$[3]. La catena ascendente $I_0 \subseteq I_1 \subseteq \ldots \subseteq I_i \subseteq I_{i+t} \subseteq \ldots$ di ideali di A, essendo noetheriano, è stazionaria: diciamo che si stabilizza in $I_{i_0} \forall i = 0, 1, \ldots, i_0$.

Scegliamo dunque un insieme finito di polinomi $f_{ij} \in I[x]$ aventi grado i e tali che i loro coefficienti direttivi a_{ij} generino I_i. Proviamo che l'insieme $\{f_{ij}\}$ genera $I[x]$. Sia $0 \neq g \in I[x]$. Supponiamo che g abbia grado d e coefficiente direttore $a \in A$ e poniamo $i = \min\{d, i_0\}$. Allora $a \in I_i$: dunque si può scrivere nella forma:

$$a = \sum_i c_j a_{ij} \quad \text{con } c_j \in A$$

Notiamo che il polinomio $g_1 = g - x^{d-i} \sum c_j f_{ij}$ di grado inferiore a d ($\deg g_1 < d$), poichè il coefficiente di x^d è nullo nel polinomio g, e dunque $g_1 \in I[x]$. Scriviamo allora $g = g_1 + x^{d-i} \sum c_j f_{ij}$: se $g_1 \neq 0$, si itera la procedura di g_1 ottenengo g_2 e così via. Dopo un numero s finito di passi, si arriva a g_s polinomio nullo.

Poichè

$$\begin{aligned} g &= g_1 + (\text{polinomio in } \langle f_{ij}\rangle) = g_2 + (\text{polinomio in}\langle f_{ij}\rangle) \\ &= g_s + (\text{polinomio in}\langle f_{ij}\rangle) = 0 + (\text{polinomio in}\langle f_{ij}\rangle) \\ &\Rightarrow g \in \langle f_{ij}\rangle \end{aligned}$$

Si conclude che $I[x] \equiv \langle f_{ij}\rangle$. □

Corollario 2.0.1. *A noetheriano, allora $A[x_1, \ldots, x_n]$ noetheriano.*

Dimostrazione. Per induzione su n.
Per $n = 1$ è il teorema (2.0.1)di Hilbert. Ipotesi induttiva su $n-1$, per n si ha:

$$A[x_1, \ldots, x_n] = A[x_1, \ldots, x_{n-1}][x_n]$$

□

Corollario 2.0.2. *A noetheriano e sia $A \hookrightarrow B$ con $u_1, \ldots, u_n \in B \Rightarrow A[u_1, \ldots, u_n]$ è noetheriano.*

[3]infatti se $f(x) = ax^i + \ldots + a_1x + a_0 \in I[x]$ anche $xf(x) = ax^{i+1} + \ldots + a_1x^2 + a_0x \in I[x]$, dunque $a \in I_i \Rightarrow a \in I_{i+1}$

Casi particolari:

- $A = \mathbb{K}$ campo: ogni campo è banalmente noetheriano perchè gli unici ideali sono quelli generati da 0 e il campo stesso (cioè l'ideale generato dall'unità)
- $A = PID$, allora $A[x]$ è noetheriano.

CAPITOLO 3

Estensioni di campi

Dato B un anello e A un sottoanello di B, si ha l'inclusione canonica: $A \hookrightarrow B$. Sia $U \subseteq B$ allora $A[U]$ è il sottoanello di B generato da $A \cup U$.

Consideriamo il caso semplice in cui $U = \{u\}$ e dunque $A[u] = \{a_n u^n + \ldots + a_1 u + a_0 \mid n \in \mathbb{N}_0; a_i \in A\}$ e sia $\Phi\colon A[x] \to A[u]$ l'omomorfismo di valutazione. Supponiamo che A sia un campo e che $A = F$. Allora $\ker \Phi$ è un ideale principale e $\ker \Phi = (g(x))$: poichè $\ker \Phi \cap F = \{0_F\}$, allora $g(x)$ non è un elemento unitario di $F[x]$ per tanto esistono due possibilità:

(1) $g(x)$ è il polinomio nullo (ho l'iniettività di Φ);
(2) $\deg g(x) > 0$.

Nel caso (1) u è trascendente su F e $F[x] \simeq F[u]$, nel caso (2)u è algebrico su F. Se si sceglie $g(x)$ monico si dirà che $g(x)$ è il polinomio minimo di u su F

Allora

$$F[u] \simeq \frac{F[x]}{(g(x))}$$

e vale la seguente:

Proposizione 3.0.4. *$F[u] \simeq \frac{F[x]}{(g(g))}$ è un campo $\Leftrightarrow$ $g(x)$ è irriducibile in $F[x]$.*

Nota 3.0.3. Se $g(x)$ è riducibile, $F[u]$ non è nemmeno un dominio.

3.1. Estensioni semplici di campi

Sia $F \subseteq E$ un'estensione di campi e sia $U = \{u\} \subseteq E$. Consideriamo $F(u) =$ {sottocampo di E generato da F e dall'elemento $u \in E$} e $F[u] =$ {sottoanello generato da F e da u} un dominio.

Considerando la classificazione precedente rispetto al $\ker \Phi$ nei casi (1) e (2), possiamo dare la seguente:

Definizione 3.1.1. Sia $F \subseteq E$ un'estensione di campi. Si dice che E è un'**estensione semplice** di F se esiste $u \in E$ tale che $E = F(u)$.

Equivalentemente si può dire:

Data $F \subseteq E$ un'estensione di campi, sia $u \in E$. L'estensione $F(u)$ si dice **semplice**.

Le estensioni semplici posso essere classificate in due categorie:

- estensioni **algebriche**, se u è algebrico su F;
- estensioni **trascendenti,** se u è trascendente su F. Questo implica che $F(u)$ sarà il campo delle funzioni razionali.

3.2. Estensione di campi come spazio vettoriale. Grado di un'estensione

Sia F un sottocampo di E. Si può considerare in modo naturale come spazio vettoriale su F, definendo come somma dello spazio vettoriale la somma nel campo e come prodotto esterno $f \cdot e$, con $f \in F, e \in E$ l'ordinario prodotto definito in E.

Definizione 3.2.1. Scriveremo

$$[E : F] = \dim_F E$$

per intendere la **dimensione di E su F** e diremo che $[E : F]$ è il **grado** dell'estensione E su F. Diremo, inoltre, che un'estensione è **finita** se $[E : F] < +\infty$.

Proposizione 3.2.1. ***(Caratterizzazione delle estensioni algebriche semplici come estensioni finite):***
Sia $u \in E$ è algebrico su $F \Leftrightarrow [F(u) : F] < +\infty$ e in tal caso $[F(u) : F]$ coincide con il grado del polinomio minimo di u su F.

Dimostrazione. ($\Rightarrow$) Supponiamo u sia algebrico su F. Sia $g(x)$ il suo polinomio minimo e deg $g(x) = n$. Allora $F(u) \simeq F[u]$ e questo significa che ogni elemento V del campo $F(u)$ è esprimibile come un polinomio in u:

$$V = a_m x^m + \ldots + a_1 x + a_0 = f(u) \in F[u]$$

Dividendo $f(x)$ per $g(x)$ si ottiene: $f(x) = q(x)g(x) + r(x)$, con $q(x)$ quoziente e $r(x)$ resto e per tanto deg $g(x) >$ deg $r(x)$. Allora:

$$\begin{aligned} V &= q(u)g(u) + r(u) \\ &= 0 + r(u) \end{aligned}$$

Quindi V è esprimibile come un polinomio di grado minore di n:

$$V = b_{n-1}u^{n-1} + \ldots + b_1 u^1 + b_0 = r(u)$$

Si conclude che $\{1, u, u^2, \ldots, u^{n-1}\} \in F(u)$ sono una base per lo spazio E sul campo F. Infatti $\{1, u, u^2, \ldots, u^{n-1}\}$ genera $F(u)$ e $\{1, u, u^2, \ldots, u^{n-1}\}$ è un'insieme di elementi linearmente indipendenti su F. In caso contrario esisterebbe una relazione lineare non banale a coefficienti in F tale per cui:

$$c(u) = c_{n-1}u^{n-1} + \ldots + c_1 u + c_0 = 0$$

Quindi $c(x)$ avrebbe radice u e grado minore di n, contro il fatto che il polinomio minimo abbia deg $g(x) = n$.

Si conclude che il grado di $F(u)$ è il grado di $g(x)$ e per tanto: $[F(u) : F] = n < +\infty$.

($\Leftarrow$) Sia u un elemento trascendente su F. Allora $\{1, u, u^2, \ldots, u^i, u^{i+1}, \ldots\}$ sono elementi indipendenti su F. Se, per assurdo, fossero dipendenti si avrebbe una relazione lineare non banale del tipo:

$$\sum_{i=0}^{R} \alpha_i u^i = 0$$

con gli α_i tutti non nulli per qualche opportuno R. Ma allora u sarebbe radice del polinomio non nullo $\sum_{i=0}^{R} \alpha_i x^i \neq 0$ e per tanto u sarebbe algebrico su F. Contraddizione.

Quindi $\{1, u, u^2, \ldots, u^i, u^{i+1}, \ldots\}$ sono indipendenti su F e non trovo in F alcun insieme massimale indipendente finito, cioè: $[F(u) : F] = +\infty$. □

Teorema 3.2.1. *(Formula dei Gradi):*
Siano $F \subseteq E \subseteq K$ estensioni di campi [1]*. Supponiamo che K sia un'estensione finita su F, cioè $[K : F] < \infty$, allora anche $[K : E] < \infty$ e $[E : F] < \infty$. Inoltre si ha:*

$$[K : F] = [K : E] \cdot [E : F]$$

Dimostrazione. Chiaramente $[E : F] < \infty$ in quanto E sottospazio di K.

Essendo $[K : F] < \infty$ per ipotesi, deve esistere una base finita $\mathcal{B}$ di K su F. Questo significa che ogni elemento di K può essere scritto come combinazione lineare di elementi della base $\mathcal{B}$ a coefficienti in F. Siccome $F \subseteq E$, questi coefficienti possono essere visti come elementi di E. Risulta che gli elementi di K sono combinazione lineare di elementi di $\mathcal{B}$ a coefficienti in E. Allora $\mathcal{B}$ è un insieme di generatori per K su E, da cui può essere estratta una base finita per K in E: $[K : E] < \infty$.

Poniamo ora $[E : F] = r$ e $[K : E] = s$. Siano $\mathcal{R} = \{x_1, \ldots, x_r\}$ una base per E su F e sia $\mathcal{S} = \{y_1, \ldots, y_s\}$ una base per K su E. Allora $\forall k \in K$ si può scrivere:

$$k = \sum_{i=1}^{s} \alpha_i y_i$$

con $\alpha_i \in E$. A sua volta, ognuno degli α_i si scrive come:

$$\alpha_i = \sum_{j=1}^{r} \beta_{ij} x_j$$

con $\beta_{ij} \in F$. Allora possiamo riscrivere l'elemento $k \in K$ come:

$$k = \sum_{i=1}^{s} \sum_{j=1}^{r} \beta_{ij} x_j y_i$$

cioè gli elementi $(x_j y_i)$ generano K su F e quindi $[K : F] \leq rs$. Vale l'uguale se $\{x_j y_i\}$ sono tutti linearmente indipendenti. Allora:

$$\sum_{i=1}^{s} \sum_{j=1}^{r} \xi_{ij}(x_j y_i) = 0$$

con ξ_{ij} non tutti nulli. Ma $\{y_i\}$ sono una base per K su E, e quindi sono tutti linearmente indipendenti su E. Allora $\sum_{j=1}^{r} \xi_{ij} x_j = 0$. Analogamente, gli $\{x_j\}$ sono una base per E su F e quindi sono tutti linearmente indipendenti su F, cioè

$$\xi_{ij} = 0 \quad \forall i, j$$

cioè $\{x_j y_i\}$ sono linearmente indipendenti e, pertanto, costituiscono una base per K su F. In particolare vale:

$$[K : F] = s \cdot r = [K : E] \cdot [E : F]$$

□

Esercizio 3.2.1. Siano $F \subseteq E$ estensione di campi. Se $U, V \subseteq E$ sottoinsiemi di E, allora $F(U \cup V) = (F(U))(V)$.

[1] E è un campo intermedio

Definizione 3.2.2. Diremo che un'estensione E di un campo F è una **estensione algebrica** se ogni elemento di E è algebrico su F.

Lemma 3.2.1. *Ogni estensione finita è algebrica.*

Dimostrazione. Sia $[E : F] < \infty$. Allora esiste una base finita $\{v_1, \dots, v_m\}$ dello spazio E sul campo F [2].

Sia $0 \neq v \in E$, allora l'insieme $\{1, v, \dots, v^m\}$ è un'insieme linearmente indipendente su F. Segue che esistono $a_0, a_1, \dots, a_m \in F$ non tutti nulli tali che

$$\sum_{i=0}^{m} a_i v^i = 0$$

e v è radice del polinomio $f(x) = \sum_{i=0}^{m} a_i x^i \in F[x]$. Si conclude che ogni elemento di E è algebrico su F. Allora E è un'estensione algebrica di F. □

Nota 3.2.1. Non è vero il viceversa, cioè che ogni estensione algebrica è finita.

Si ha la seguente caratterizzazione delle estensioni:

Lemma 3.2.2. $[E : F] < \infty \iff$ *esistono* $u_1, \dots, u_n \in E$ *algebrici su F tali che* $E = F(u_1, \dots, u_n)$.

Dimostrazione. ($\Rightarrow$) Supponiamo che $[E : F] = n < \infty$. Allora esiste una base $\{u_1, \dots, u_n\}$ per E come spazio vettoriale su F. Poichè E è algebrica per il lemma (3.2.1), allora gli u_i sono algebrici su F $\forall i = 1, \dots, n$.

($\Leftarrow$) Supponiamo che $E = F(u_1, \dots, u_n)$ con $u_i \in E$ $\forall i$ e gli u_i sono algebrici su F $\forall i = 1, \dots, n$.

Proviamo che $[E : F] < \infty$ per induzione su n:

- $n = 1$: $E = F(u_1)$ con u_1 algebrico. Questa è un'estensione semplice mediante un elemento algebrico, quindi è un'estensione finita, con $[E : F] = m$ ove $m = \deg(g(x))$ con $g(x)$ polinomio minimo di u_1 su F.
- Ipotesi induttiva per $n - 1$: $E = F(u_1, \dots, u_{n-1}) \Rightarrow [E : F] < \infty$.
- n: $F(u_1, \dots, u_n) = F(u_1, \dots, u_{n-1})(u_n)$ quindi per l'ipotesi induttiva si ha che $[F(u_1, \dots, u_n) : F] < \infty$. Inoltre, se poniamo $H = F(u_1, \dots, u_{n-1})$, vediamo che, essendo u_n algebrico su F è a maggior ragione algebrico su H. Allora $[F(u_1, \dots, u_n) : H] < \infty$. Quindi per la formula dei gradi:

$$[E : F] = [E : H] \cdot [H : F] < \infty$$

□

Osservazione 3.2.1. Sia

$$\mathbb{A} = \{\text{insieme di tutti i numeri complessi algebrici su } \mathbb{Q}\}$$

l'insieme dei numeri algebrici. Possiamo osservare che:

- $\mathbb{A}$ è un sottocampo di $\mathbb{C}$.

  Siano $\alpha, \beta \in \mathbb{A}$ tali che: $[\mathbb{Q}(\alpha) : \mathbb{Q}] < +\infty$ e $[\mathbb{Q}(\beta) : \mathbb{Q}] < +\infty$. Segue che se estendo $\mathbb{Q}(\alpha)$ mediante β ottengo $[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}(\alpha)] < +\infty$. Allora $[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}(\alpha)] \cdot [\mathbb{Q}(\alpha) : \mathbb{Q}] = [\mathbb{Q}(\alpha, \beta) : \mathbb{Q}] < +\infty$, cioè $\mathbb{Q}(\alpha, \beta)$ è un'estensione algebrica su $\mathbb{Q}$. Questo significa che $\alpha - \beta \in \mathbb{Q}(\alpha, \beta) \Rightarrow \alpha - \beta$ è algebrico su $\mathbb{Q}(\alpha, \beta)$. Analogamente: $\alpha\beta^{-1} \in$

[2] ovviamente $E = F(v_1, \dots, v_m)$.

$\mathbb{Q}(\alpha,\beta) \Rightarrow \alpha\beta^{-1}$ è algebrico su $\mathbb{Q}(\alpha,\beta)$. Ma $\alpha,\beta \in \mathbb{A} \Rightarrow \alpha-\beta, \alpha\beta^{-1} \in \mathbb{A} \Rightarrow \mathbb{A}$ è un sottocampo di $\mathbb{C}$.

- $[\mathbb{A}:\mathbb{Q}] = \infty$ è un'estensione algebrica infinita poichè se $[\mathbb{A}:\mathbb{Q}] = m < \infty$ ogni elemento di $\mathbb{A}$ sarebbe algebrico su $\mathbb{Q}$ con un polinomio minimo di grado $\leq m$. Ma esistono polinomi irriducibili in $\mathbb{Q}[x]$ di grado arbitrario.
- $\mathbb{A}$ è algebricamente chiuso, infatti è la chiustura algebrica di $\mathbb{Q}$[3].

Proposizione 3.2.2. *Sia $K \subseteq E \subseteq F$ e siano $K \subseteq E$ e $E \subseteq F$ estensioni algebriche di campi. Allora $K \subseteq F$ è un'estensione algebrica di campi.*

Dimostrazione. Sia $u \in K \Rightarrow u$ è radice di un polinomio $f(x) \in E[x]$: $f(x) = \sum_{i=0}^{n} a_i x^i$. D'altronde gli $a_i \in E\ \forall i = 0,\dots,n$, allora gli a_i sono algebrici su F.

Posto $H = F(a_0, a_1, \dots, a_n)$ estensione di F mediante n elementi di E [4]. Allora $[H:F] < \infty$ estensione di grado finito poichè il campo F è stato esteso mediante un numero finito di elementi algebrici.

Poichè $\forall i\ a_i \in H$, u è algebrico su H e per tanto: $[H(u):H] < \infty$. Allora per la formula dei gradi:

$$[H(u):F] = [H(u):H]\cdot[H:F] < \infty$$

Ma ogni estensione finita è algebrica, per tanto u è algebrico su F.Ma u è un generico elemento di K$\Rightarrow$ K algebrico su F. □

Lemma 3.2.3. *$\mathbb{A}$ è algebricamente chiuso.*

Dimostrazione. Si deve dimostrare che ogni polinomio a coefficienti in $\mathbb{A}$ ha almeno una radice in $\mathbb{A}$ (e quindi per Ruffini ha tutte le radici in $\mathbb{A}$).

Sia $0 \neq f(x) \in \mathbb{A}[x]$ Per il teorema fondamentale dell'algebra [5], $\exists \alpha \in \mathbb{C}$ tale che $f(\alpha) = 0$. Duqnue α è un elemento algebrico su $\mathbb{A}$, allora $\mathbb{A}(\alpha)$ è un'estensione algebrica di $\mathbb{Q}$. Per la proposizione (3.2.2) $\mathbb{A}(\alpha)$ è un'estensione algebrica di $\mathbb{Q}$, cioè α è algebrico su $\mathbb{Q} \Rightarrow \alpha \in \mathbb{A}$.

Ogni radice complessa di $f(x) \in \mathbb{A}[x]$ appartiene ad $\mathbb{A}$, allora $\mathbb{A}$ è algebricamente chiuso. □

Definizione 3.2.3. Gli **interi algebrici** sono i numeri complessi che sono radici di un polinomio monico a coefficienti interi.

Nota 3.2.2. L'insieme degli interi algebrici è un anello. Ogni intero algebrico che sia razionale è un intero.

3.3. Campo di spezzamento di un polinomio a coefficienti su un campo

Definizione 3.3.1. Sia F un campo e $F[x]$ l'anello dei polinomio in x a coefficienti sul campo F.

Sia, inoltre, $f(x) \in F[x]$ deg $f(x) = n > 0$. Si dice **campo di spezzamento** per $f(x)$ su F un'estensione E di F tale che:

(1) $f(x)$ si spezzi in fattori lineari su E, cioè

$$f(x) = c(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n)$$

con gli $\alpha_i \in E\ \forall i = 1,\dots,n$;

[3] $\mathbb{A}$ è il più piccolo sottocampo di $\mathbb{C}$ algebricamente chiuso.

[4] tutti gli n elementi sono algebrici su E e sono un numero finito di elementi

[5] $\mathbb{C}$ è algebricamente chiuso.

(2) $E = F(\alpha_1, \alpha_2, \ldots, \alpha_n)$. E si ottiene estendendo F mediante $\alpha_1, \alpha_2, \ldots, \alpha_n$[6].

NOTA 3.3.1. Nel punto (2) si ha che E è estensione di F mediante un numero finito di elementi algebrici su F: $[E : F] < \infty$.

3.3.1. Esistenza del campo di spezzamento.
L'ingrediente base per dimostrare l'esistenza è la seguente:

PROPOSIZIONE 3.3.1. *Sia $f(x) \in F[x]$ monico e irriducibile su F, allora esiste una estensione semplice di F mediante un elemento di α : $E = F(\alpha)$ tale che:*

- $f(\alpha) = 0$*;*
- $f(x)$ *è il polinomio minimo di* α su F[7]*.*

DIMOSTRAZIONE. Sia $(f(x)) = I$ l'ideale massimale e si consideri il campo $K = \frac{F[x]}{(f(x))} = \frac{F[x]}{I}$. L'applicazione $a \overset{\varphi}{\mapsto} I + a$ con $a \in F, I + a \in K$. φ è un monomorfismo di F in K[8].

Identificando F con $\varphi(F)$ si può vedere K come estensione di F e pensare $f(x) \in K[x]$. Si ponga $\alpha = I + x$. Allora si ha che

$$f(\alpha) = f(I + x) = I + f(x) = I$$

che è lo zero di K. Dunque in $K[x]$:$f(\alpha) = 0$. Allora α è radice di $f(x)$ in K. Inoltre $f(x)$ è il polinomio minimo di α su F, poichè $f(x)$ è irriducibile e monico su F. Se $f(x)$ non fosse il polinomio minimo, esisterebbe $g(x)$ polinomio minimo. Ma in quel caso: $\deg g(x) < \deg f(x)$ e quindi $g(x)$ fattore proprio di $f(x)$. Assurdo, poichè $f(x)$ irriducibile.

Infine, dunque, $K = F(\alpha)$. Sappiamo infatti che $F(\alpha)$ è un'estensione semplice con α algebrico su F ed è isomorfa precisamente all'anelo quoziente $\frac{F[x]}{(\delta(x))}$ con $\delta(x)$ polinomio minimo di α su F. □

Possiamo a questo punto enunciare e dimostrare il seguente:

TEOREMA 3.3.1. *Per ogni campo F e $\forall f(x) \in F[x]$ di grado positivo, esiste un campo di spezzamento per $f(x)$ su F.*

DIMOSTRAZIONE. Per induzione sul grado di $f(x)$:

- $\deg f(x) = 1$: il campo di spezzamento è lo stesso F;
- $\deg f(x) > 1$: ci sono due possibilità: $f(x)$ si spezza su F, quindi F è il campo di spezzamento, oppure $f(x)$ non si spezza su F. In questo caso $f(x)$ ammette in $F[x]$ un fattore irriducibile $f_1(x)$ con $\deg f_1(x) > 1$. Per la proposizione (3.3.1)esiste una estensione semplice di $F[\alpha_1]$ di F tale che α_1 sia radice di $f_1(x)$ e quindi α_1 è anche radice di $f(x)$. Allora $f_1(\alpha) = 0 \Rightarrow f(\alpha) = 0$.

  Dunque nell'anello dei polinomio $F(\alpha_1)[x]$ si ha:

  $$f(x) = (x - \alpha_1)g(x)$$

  dove $\deg g(x) < \deg f(x)$, in particolare $\deg g(x) = \deg f(x) - 1$.

  Per induzione sul grado, $g(x)$ ammette un campo di spezzament su $F(\alpha_1)$. C'è un'estensione di $F(\alpha_1)$ che contiene tutte le radici di $g(x)$:

[6]E è la più piccola estensione di F che contiene tutte le radici di $f(x)$.
[7]per questo motivo necessitiamo $f(x)$ sia monico
[8]$\ker \varphi = 0$

chiamiamo questa estensione $\Sigma = F(\alpha_1)(\alpha_2, \ldots, \alpha_j)$. Allora Σ è anche un campo di spezzamento per $f(x)$ su F.

□

3.3.2. Unicità del campo di spezzamento.
Premettiamo il seguente:

Lemma 3.3.1. *Sia $\eta : F \to F_1$ con $F \simeq F_1$ campi isomorfi. Siano $u \in F, v \in F_1$ elementi algebrici rispettivamente di F e di F_1 con polinomi minimi $m_u(x) \in F[x]$ e $m_v(x) \in F_1[x]$. Si consideri l'isomorfismo $\hat{\eta}\colon F[x] \to F_1[x]$ definito da*

$$f(x) = \sum_{i=0}^{m} a_i x^i \mapsto \sum_{i=0}^{m} \eta(a_i) x^i$$

Si supponga che $\hat{\eta}(m_u(x)) = m_v(x)$. Allora η si estende in modo unico ad un isomorfismo di campi $\eta_1\colon F(u) \to F_1(u)$ tale che $\eta_1(u) = v$.

Dimostrazione. Sia $\deg m_\mu(x) = n$. Allora $[F(u) : F] = [F_1(u) : F_1] = n$. Sappiamo che ogni elemento di $F(u)$ si può scrivere in modo unico nella forma

$$f(u) = a_{n-1}u^{n-1} + \ldots + a_1 u + a_0$$

Similmente ogni elemento di $F_1(u)$ si scrive in modo unico come un polinomio in v a coefficienti in F_1 di grado $\leq n-1$. Sia η_1 l'applicazione

$$f(u) = a_{n-1}u^{n-1} + \ldots + a_1 u + a_0 \mapsto \eta(a_{n-1})u^{n-1} + \ldots + \eta(a_1)u + \eta(a_0) = \hat{\eta}(f)(v)$$

Allora η_1 è ben definita e biettiva. Inoltre $\eta_1 \mid_F \equiv \eta$ e $\eta_1(u) = v$. É anche chiaro che η_1 conserva la somma. Ricordando che $1_{F(u)} = 1_F, 1_{F_1(v)} = 1_{F_1}$ si ha anche $\eta_1(1_{F(u)}) = 1_{F_1(v)}$.

Conservazione del prodotto: siano $f(u), g(u) \in F(u)$ in forma canonica e sia $h(u) = f(u)g(u)$[9]. Poichè $f(u)g(u) - h(u) = 0$, $f(x)g(x) - h(x) = 0$ è divisibile per $m_u(x)$, in quanto u radice di $f(x)g(x) - h(x)$.

Sia $f(x)g(x) - h(x) = m_u(x)q(x)$. Allora $\hat{\eta}(f(x)g(x) - h(x)) = (\hat{\eta}f)(x)(\hat{\eta}g)(x) - (\hat{\eta}h)(x) = m_v(x)(\hat{\eta}q)(x)$.Segue, essendo $m_v(v) = 0$, che $(\hat{\eta}f)(v)(\hat{\eta}g)(v) = (\hat{\eta}h)(v)$,dunque:

$$f(u)g(u) = h(u) \overset{\eta_1}{\mapsto} (\hat{\eta}h)(u) = (\hat{\eta}f)(v) \cdot (\hat{\eta}g)(v) = \hat{\eta}_1(f(u)) \cdot \hat{\eta}_1(g(u))$$

□

Lemma 3.3.2. *Sia $\eta\colon F \to F_1$ un isomorfismo di campi e u, v algebrici su F, F_1 rispettivamente. Dati $m_v(x) = \hat{\eta}(m_u(x))$ allora $\hat{\eta}\colon F[x] \to F_1[x]$ con $\hat{\eta} \mid_F = \eta$. Allora η si estende in modo unico ad un isomorfismo*

$$\eta_1\colon F(u) \to F_1(u)$$

con $\eta_1(u) = v$.

Teorema 3.3.2. *Sia $\eta\colon F \to F_1$ un isomorfismo di campi. Sa $f(x) \in F[x]$ e sia E un campo di spezzamento per $f(x)$ su F. Sia E_1 un'estensione qualsiasi di F_1 tale che il polinomio $\hat{\eta}(f(x))$ si spezzi su E_1. Allora esiste un monomorfismo $\xi\colon E \to E_1$ che estende η, cioè tale che $\xi \mid_F = \eta$.*

[9] $h(u)$ in forma canonica significa che $\deg h(x) \leq n-1$.

DIMOSTRAZIONE. La dimostrazione è per induzione sul grado di $f(x)$.

$$\begin{array}{ccc} F & \xrightarrow{\eta} & F_1 \\ \subseteq\big\downarrow & & \big\downarrow\subseteq \\ E & \xrightarrow{\xi} & E_1 \end{array} \tag{3.3.1}$$

- Sia $\deg f(x) = 1$. Si ha che $f(x) = c(x-\alpha)$. $f(x)$ si spezza su F, allora $E \equiv F$. Se considero $\hat{\eta}(f(x)) = \eta(c)(x - \eta(\alpha))$, allora $\hat{\eta}(f(x))$ si spezza su F_1. Quindi per ogni scelta di E_1 l'applicazione η funziona come ξ.
- sia $\deg f(x) > 1$. In $E[x]$ si ha che:

  $$f(x) = c(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_m)$$

  con $\deg f(x) = m$. Il polinomio minimo di α_1 su F (è un divisore di $f(x)$) è un fattore irriducibile in F di $f(x)$: sia esso $m(x)$. Allora $\hat{\eta}(m(x))$ è un fattore di $\hat{\eta}(f(x))$ che si spezza in fattori lineari in $E_1[x]$. In $E_1[x]$ si ha che:

  $$\hat{\eta}(m(x)) = \prod_{i=1}^{r}(x-\beta_i)$$

  ove $\beta_i \in E_1$ e $r \leq m$. D'altronde $m(x)$ è irriducibile su F, quindi anche $\hat{\eta}(m(x))$ è irriducibile su F_1 Allora

  $$\hat{\eta}(m(x)) = \prod_{i=1}^{r}(x-\beta_i)$$

  è il polinomio minimo di β_1 su F_1[10]. Scegliendo quindi come $u, v \longrightarrow \alpha_1, \beta_1$ possiamo applicare il lemma (3.3.2) η si estende ad un isomorfismo $\eta_1 \colon F(\alpha_1) \to F_1(\beta_1)$ tale che $\eta_1(\alpha_1) = \beta_1$. Poniamo ora $f(x) = (x-\alpha_1)g(x)$ e sia $E = F(\alpha_1, \ldots, \alpha_m) = F(\alpha_1)(\alpha_2, \ldots, \alpha_m)$ per definizione di campo di spezzamento. Scrivendo così vediamo che E è un campo di spazzamento per $g(x)$ su $F(\alpha_1)$. Per ipotesi induttiva, esiste un monomorfismo $\xi \colon E \to E_1$ tale che $\xi \mid_{F(\alpha_1)} = \eta_1$[11]. Poichè $\eta \mid_F = \eta$, a maggior ragione: $\xi \mid_F = \eta$.

□

COROLLARIO 3.3.1. *Nelle ipotesi del teorema* (3.3.2)*, se si prende per E_1 un campo di spezzamento*[12] *per $\hat{\eta}(f(x))$ su F_1, allora il monomorfismo $\xi \colon E \to E_1$ è un isomorfismo.*

DIMOSTRAZIONE. Basta osservare che $\xi(E)$ è un campo di spezzamento per $\hat{\eta}(f(x))$ su F_1 e $\xi(E) \subseteq E_1$. Per ipotesi, E_1 è anch'esso un campo di spezzamento per $\hat{\eta}(f(x))$ su F_1, allora deve essere $\xi(E) \equiv E_1$, allora ξ suriettiva e per tanto ξ isomorfismo. □

[10] è il polinomio minimo di ognuno dei β_i ma ne scegliamo uno: per comodità il primo.

[11] si noti che $\hat{\eta}(g(x))$ si spezza su E_1

[12] non un qualsiasi campo su cui si spezzi

Osservazione 3.3.1. Il teorema (3.3.2) è un teorema di unicità a meno di isomorfismi nel senso che se $F = F_1$ e $\eta = Id$ allora il corollario (3.3.1)afferma che, comunque siano ottenuti, due campi di spezzamento per un polinomio $f(x) \in F[x]$ sono necessariamente isomorfi.

Esempio 3.3.1. (Caso banale) :
Sia $f(x) = x^2 + ax + b \in F[x]$. Allora ho due possibilità:

- $f(x)$ è irriducibile su F, allora F è un campo di spezzamento per $f(x)$.
- $f(x)$ è riducibile su F, allora $\frac{F[x]}{(f(x))} = E = F[\alpha]$ ove $\alpha = (f(x)) + x$. Allora E sarà un campo di spezzamento per $f(x)$ con $[F(\alpha) : F] = 2$.

3.4. Derivazione formale e radici multiple

Sia F un campo e $f(x) \in F[x]$ un polinomio della forma:

$$f(x) = a_n x^n + \cdots + a_1 x + a_0$$

Definizione 3.4.1. Definiamo derivata formale di f il polinomio

$$f'(x) = n a_n x^{n-1} + \cdots + 2a_2 x + a_1$$

Questa derivata formale gode delle stesse proprietà di calcolo dell'usuale derivata di funzioni $\mathbb{R} \to \mathbb{R}$:

(1) (F- linearità): $(\alpha f + \beta g)' = \alpha f' + \beta g' \quad \text{con} \quad \alpha, \beta \in F$;
(2) (Regola del prodotto): $(fg)' = f'g + fg'$.

Lemma 3.4.1. *Sia $f(x) \in F[x]$ di grado positivo. $f(x)$ ammette una radice multipla (di molteplicità >1) in un qualsiasi campo di spezzamento se e solo se $MCD(f(x), f'(x))$ ha grado maggiore di zero.*

Dimostrazione. ($\Rightarrow$) sia α una radice multipla di $f(x)$ in E. Allora in $E[x]$ si ha $f(x) = (x - \alpha)^2 g(x)$. Si ha che:

$$\begin{aligned} f'(x) &= 2(x - \alpha)g(x) + (x - \alpha)g'(x) \\ &= (x - \alpha)[2g(x) + (x - \alpha)g'(x)] \end{aligned}$$

in $E[x]$. Questo significa che $f(x)$ e $f'(x)$ hanno entrambi radice α in $E[x]$.

Dunque sia $f(x)$ che $f'(x)$ sono divisibili per il polinomio minimo $m(x)$ di α su F. Dunque: $m(x) \mid MCD(f(x), f'(x))$.

($\Leftarrow$) Supponiamo ora che $f(x)$ non abbia radici multiple in $E[x]$. Per induzione sul grado di $f(x)$ proveremo che f e f' sono coprimi in $E[x]$ e quindi *a fortiori* in $F[x]$. □

- Se $\deg f(x) = 1$, allora: $f(x) = a_1 x + a_0$ e $f'(x) = a_1$ e quindi $MCD(f, f') = 1$.
- Se $\deg f(x) > 1$ e sia $\alpha \in E$ una sua radice. Per l'ipotesi in $E[x]$ si avrà anche $f(x) = (x - \alpha)g(x)$ ove $\deg g(x) > 0$ e $(x - \alpha) \nmid g(x)$.

  Si ha che $f'(x) = g(x) + (x - \alpha)g'(x)$. Osserviamo che un fattore comune tra $f(x)$ e $f'(x)$ deve dividere $g(x)$, poichè se così non fosse questo fattore comune dovrebbe essere del tipo: $(x - \alpha)h(x)$. Allora

  $$f'(x) = (x - \alpha)h(x)k(x) + (x - \alpha)^2 h(x)j(x)$$

  ma questo contraddice il fatto che $(x - \alpha) \nmid f'(x)$.

  D'altra parte se un fattore di $g(x)$ divide $f'(x)$ necessariamente deve essere anche $g'(x)$, poichè deve essere coprimo con $(x - \alpha)$. Concludendo,

per l'ipotesi induttiva, $MCD(g(x), g'(x)) = 1 \Rightarrow MCD(f(x), f'(x)) = 1$ cioè non ci sono fattori di grado positivo comuni a $f(x)$ e $f'(x)$.

Definizione 3.4.2. Un polinomio $f(x) \in F[x]$, con $f(x)$ irriducibile in $F[x]$, si dice **separabile** su F se non ha radici multiple in un campo di spezzamento. In caso contrario $f(x)$ si dice **inseparabile** su F.

Proposizione 3.4.1. *Sia F un campo.*

(1) *Se* $carF = 0$*, ogni polinomio irriducibile su F è separabile;*
(2) *se* $carF = p > 0$*, un polinomio irriducibile su F è inseparabile* $\iff$ *ha la forma*

$$f(x) = a_h x^{hp} + a_{h-1} x^{(h-1)p} + \ldots + a_1 x^p + a_0$$

ovvero $f(x) = g(x^p)$ *per qualche* $g(x) \in F[x]$.

Dimostrazione. Per il lemma (3.4.1) sappiamo che $f(x)$ è separabile se e solo se f e f' hanno in comune un fattore di grado positivo. Poichè $f(x)$ è irriducibile e $\deg f'(x) < \deg f(x)$, questo accade $\Leftrightarrow f'(x) = 0$.

Poniamo $f(x) = \sum_{i=0}^{n} a_1 x^i$ e $f'(x) = \sum_{i=1}^{n} i \cdot a_{i-1} x^{i-1}$. Deve quindi essere $i \cdot a_i = 0 \; \forall i > 0$.

(1) se car$F = 0$: $na_n = 0 \Leftrightarrow a_n = 0$ poichè ogni elemento ha periodo additivo infinito. Questa è una contraddizione perchè a_n è il coefficiente direttivo di $f(x)$, quindi per definizione non nullo.
(2) Se car$F = p > 0$ e $ia_i = 0 \Rightarrow a_i = 0$ ogni qualvolta $p \nmid i$. Si conclude che $f(x)$ ha la forma:

$$f(x) = a_h x^{hp} + a_{h-1} x^{(h-1)p} + \ldots + a_1 x^p + a_0.$$

□

3.5. Campi finiti

Proposizione 3.5.1. *Sia F un campo finito. Allora* $carF = p > 0$ *e* $|F| = p^n$ *ove* $n = |F : P|$ *con* $P \simeq \frac{\mathbb{Z}}{p\mathbb{Z}}$ *è il sottocampo primo minimo di F.*

Dimostrazione. Sia $|F| < \infty$, allora car$F = p > 0$ con p primo. Sappiamo anche che $P \simeq \frac{\mathbb{Z}}{p\mathbb{Z}}$ (campo delle classi di resto modulo p). Allora F è uno spazio vettoriale di dimensione finita n su P. Sia allora $\{v_1, \ldots, v_n\}$ una base di F su P. Ogni elemento di F si scrive in un unico modo nella forma:

$$v = \lambda_1 v_1 + \ldots + \lambda_n v_n$$

con $(\lambda_i \in P)$. Segue che $|F| = p^n$. □

Definizione 3.5.1. Un campo di caratteristica $p > 0$ si dice **perfetto** se ogni elemento si può esprimere come potenza p-esima di qualche elemento.

Esempio 3.5.1. I campi algebricamente chiusi sono campi perfetti.

Lemma 3.5.1. *Sia F un campo di caratteristica p >0 e si consideri l'applicazione* $\Phi \colon F \to F$ *definita da* $a \mapsto a^n \quad \forall a \in F$*. L'applicazione* Φ *è un monomorfimo di campi e prende il nome di* ***mappa di Frobenius****.*

Dimostrazione. $\forall a, b \in F$:

– $\Phi(ab) = (ab)^p = a^p b^p = \Phi(a)\Phi(b)$;

- $\Phi(a+b) = (a+b)^p = \sum_{i=0}^{p} \binom{p}{i} a^{p-1}b^i = a^p + pa^{p-1}b + \ldots + b^p$.
  $\binom{p}{i}$ è un multiplo di p $\forall 0 < i < p$ allora è uguale a 0 in F. Allora $a^p + b^p = \Phi(a) + \Phi(b)$.
- $\Phi(1_F) = 1_F^p = 1_F \neq 0 \Rightarrow \ker\Phi = \{0_F\}$.

□

NOTA 3.5.1. Se $F = \frac{\mathbb{Z}}{p\mathbb{Z}}$ e $\Phi \equiv Id : a^p = a \; \forall a \in \frac{\mathbb{Z}}{p\mathbb{Z}}$;
Se $F = \frac{\mathbb{Z}}{p\mathbb{Z}}(\alpha)$, α è radice di $x^2 + x + 1 \in \frac{\mathbb{Z}}{p\mathbb{Z}}[x]$. Si ha che $|F| = 4$ e $\Phi \neq Id$.

TEOREMA 3.5.1. *Sia p primo e $n \in \mathbb{N}$. Un campo F ha ordine $q = p^n \Leftrightarrow F$ è un campo di spezzamento per il polinomio $x^q - x$ sul campo $P = \frac{\mathbb{Z}}{p\mathbb{Z}}$ (sottocampo minimo di F).*

DIMOSTRAZIONE. ($\Rightarrow$) Sia $|F| = qp^n$ e sia $(F, \cdot)$ il gruppo moltiplicativo di F. Per il teorema di Lagrange $\forall a \in F^*, a^{q-1} = 1_F$. Posto $f(x) = x^q - x \in P[x]$, si ha che

$$f(a) = a^q - a = a^{q-1} \cdot a - a = 1_F \cdot a - a = 0 \; \forall a \in F$$

Si conclude che $x^q - x$ si spezza su F perchè è un polinomio di grado q avente come radice tutti gli elementi di F, quindi ha q radici distinte in F.

($\Leftarrow$) Inversamente supponiamo che F sia un campo di spezzamento per $x^q - x$ su $P = \frac{\mathbb{Z}}{p\mathbb{Z}}$. Dato $f(x) = x^q - x$, si ha:

$$f'(x) = qx^{q-1} - 1 = p^n x^{p^n - 1} - 1 = -1$$

Allora $f(x)$ è coprimo con $f'(x)$ e pertanto $f(x)$ non ammette radici multiple. Allora $f(x)$ è separabile in $\frac{\mathbb{Z}}{p\mathbb{Z}}$ e quindi $f(x)$ ha $q = p^n$ radici distinte in F.

Diciamo che l'insieme di tali radici è un sottocampo di F. Siano infatti α, β due tali radici:

- $(\alpha, \beta)^q = (\alpha\beta)^{p^n} = \Phi^n(\alpha\beta) = \Phi^n(\alpha)\Phi^n(\beta) = \alpha^{p^n}\beta^{p^n} = \alpha^q\beta^q$. Ma se α, β sono radici di $x^q - x$ si ha che $\alpha^q - \alpha = 0$, cioè $\alpha^q = \alpha$ e $\beta^q - \beta = 0 \Rightarrow \beta^q = \beta$, quindi $(\alpha\beta)^q = \alpha^q\beta^q = \alpha\beta$.
- Similmente si vede che $(\alpha - \beta)^q = (\alpha - \beta)^{p^n} = \Phi^n(\alpha - \beta) = \alpha^{p^n} - \beta^{p^n} = \alpha^q - \beta^q = \alpha - \beta$.
- $\forall \alpha \neq 0 : \quad (\alpha^{-1})^q = (\alpha^q)^{-1} = \alpha^{-1}$.

Si conclude che, essendo F di spezzamento per $f(x)$ su P per ipotesi, allora F deve coincidere con l'insieme delle q radici di $x^q - x$. Per tanto $|F| = q$. □

COROLLARIO 3.5.1. *Per ogni $q = p^n$ con p primo, esiste, a meno di isomorfismi, un unico campo finito F tale che $|F| = q$. F è costruibile come campo di spezzamento del polinomio $f(x) = x^q - x$ su $\frac{\mathbb{Z}}{p\mathbb{Z}}$.*

DIMOSTRAZIONE. Basta ricordare che il campo di spezzamento di un polinomio è unico a meno di isomorfismi.

□